

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/002514

International filing date: 10 February 2005 (10.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-033355
Filing date: 10 February 2004 (10.02.2004)

Date of receipt at the International Bureau: 31 March 2005 (31.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

10. 2. 2005

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 2 月 1 0 日

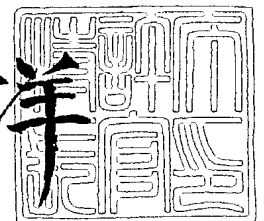
出 願 番 号
Application Number: 特 願 2 0 0 4 - 0 3 3 3 5 5
[ST. 10/C]: [J P 2 0 0 4 - 0 3 3 3 5 5]

出 願 人
Applicant(s): エヌ・ティ・ティ・コミュニケーションズ株式会社

2 0 0 5 年 3 月 1 7 日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋



【書類名】 特許願
【整理番号】 GLN-00470
【提出日】 平成16年 2月10日
【あて先】 特許庁長官殿
【国際特許分類】 G09C 1/00
【発明者】
 【住所又は居所】 東京都千代田区内幸町一丁目 1 番 6 号 エヌ・ティ・ティ・コ
 ミュニケーションズ株式会社内
 【氏名】 加賀谷 誠
【発明者】
 【住所又は居所】 東京都千代田区内幸町一丁目 1 番 6 号 エヌ・ティ・ティ・コ
 ミュニケーションズ株式会社内
 【氏名】 荻原 利彦
【発明者】
 【住所又は居所】 東京都千代田区内幸町一丁目 1 番 6 号 エヌ・ティ・ティ・コ
 ミュニケーションズ株式会社内
 【氏名】 野村 進
【特許出願人】
 【識別番号】 399035766
 【氏名又は名称】 エヌ・ティ・ティ・コミュニケーションズ株式会社
【代理人】
 【識別番号】 100083806
 【弁理士】
 【氏名又は名称】 三好 秀和
 【電話番号】 03-3504-3075
【選任した代理人】
 【識別番号】 100068342
 【弁理士】
 【氏名又は名称】 三好 保男
【選任した代理人】
 【識別番号】 100095500
 【弁理士】
 【氏名又は名称】 伊藤 正和
【選任した代理人】
 【識別番号】 100101247
 【弁理士】
 【氏名又は名称】 高橋 俊一
【選任した代理人】
 【識別番号】 100098327
 【弁理士】
 【氏名又は名称】 高松 俊雄
【手数料の表示】
 【予納台帳番号】 001982
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9908855

【書類名】 特許請求の範囲**【請求項 1】**

利用者の機密情報を管理する機密情報管理システムであって、
前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割手段と、

前記複数の分割データの一部を、前記利用者が保持するための分割データとして第 1 の記憶部に記憶させるとともに、前記複数の分割データの残りを、1 又は複数の第 2 の記憶部それぞれに記憶させるデータ記憶手段と、

必要に応じて前記秘密分散法を用いて、前記第 2 の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割手段で作成された分割データとは異なる複数の分割データを生成するデータ再分割手段と、

前記データ再分割手段で作成された前記複数の分割データの一部を前記第 1 の記憶部に記憶させるとともに、前記第 2 の記憶部に記憶された各分割データを無効にして、前記データ再分割手段で作成された前記複数のデータの残りを前記第 2 の記憶部それぞれに記憶させるデータ再記憶手段と、

を有することを特徴とする機密情報管理システム。

【請求項 2】

前記機密情報を使用する場合には、前記利用者が保持する分割データを取得し、該分割データと前記第 2 の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元手段を有することを特徴とする請求項 1 記載の機密情報管理システム。

【請求項 3】

前記機密情報を使用するときには、使用した事実を使用履歴情報として記憶する使用履歴記憶手段を有することを特徴とする請求項 2 記載の機密情報管理システム。

【請求項 4】

前記機密情報を使用する場合には、前記第 2 の記憶部に記憶された各分割データのうち、前記所定の個数から前記利用者が保持する分割データの個数を引いた個数の分割データの組み合わせを前記利用者が有する端末に通信ネットワークを介して送信する分割データ送信手段を有することを特徴とする請求項 1 記載の機密情報管理システム。

【請求項 5】

前記第 1 の記憶部に記憶される分割データを通信ネットワークを介して前記利用者が有する端末に送信する送信手段を有することを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の機密情報管理システム。

【請求項 6】

前記機密情報を前記利用者が有する端末から通信ネットワークを介して受信する受信手段を有することを特徴とする請求項 1 乃至 5 のいずれか 1 項に記載の機密情報管理システム。

【請求項 7】


利用者の機密情報を管理する機密情報管理方法であって、

前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割ステップと、

前記複数の分割データの一部を、前記利用者が保持するための分割データとして第 1 の記憶部に記憶させるとともに、前記複数の分割データの残りを、1 又は複数の第 2 の記憶部それぞれに記憶させるデータ記憶ステップと、

必要に応じて前記秘密分散法を用いて、前記第 2 の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割ステップで作成された分割データとは異なる複数の分割データを生成するデータ再分割ステップと、

前記データ再分割ステップで作成された前記複数の分割データの一部を前記第 1 の記憶部に記憶させるとともに、前記第 2 の記憶部に記憶された各分割データを無効にして、前



記データ再分割ステップで作成された前記複数のデータの残りを前記第 2 の記憶部それぞれに記憶させるデータ再記憶ステップと、
を有することを特徴とする機密情報管理方法。

【請求項 8】

利用者の機密情報を管理するためのコンピュータが読み取り可能な機密情報管理プログラムであって、

前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割ステップと、

前記複数の分割データの一部を、前記利用者が保持するための分割データとして第 1 の記憶部に記憶させるとともに、前記複数の分割データの残りを、1 又は複数の第 2 の記憶部それぞれに記憶させるデータ記憶ステップと、

必要に応じて前記秘密分散法を用いて、前記第 2 の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割ステップで作成された分割データとは異なる複数の分割データを生成するデータ再分割ステップと、

前記データ再分割ステップで作成された前記複数の分割データの一部を前記第 1 の記憶部に記憶させるとともに、前記第 2 の記憶部に記憶された各分割データを無効にして、前記データ再分割ステップで作成された前記複数のデータの残りを前記第 2 の記憶部それぞれに記憶させるデータ再記憶ステップと、
前記コンピュータに実行させることを特徴とする機密情報管理プログラム。

【書類名】明細書

【発明の名称】機密情報管理システム、機密情報管理方法、および機密情報管理プログラム

【技術分野】

【0001】

本発明は、利用者の機密情報を管理する機密情報管理システム、機密情報管理方法、および機密情報管理プログラムに関する。

【背景技術】

【0002】

IT (Information Technology) 技術の発展に伴って、パスワード、クレジット番号などが入った携帯電話および携帯情報端末、並びにPKI秘密鍵が入ったICカードなどを用いて、所望のサービスの提供を受ける機会が増えている。例えば、ユーザのパスワードを使用してログインし、情報を閲覧したり、ユーザのクレジットカード番号を使用して物品購入したりするようなサービスが普及している。

【0003】

このような機会において、ユーザが上述した機密情報（例えば、パスワード、クレジット番号およびPKI秘密鍵など）が記憶されている携帯電話、携帯情報端末およびICカードなどを紛失した場合には、紛失した旨を発行元に申告して、該機密情報を失効させ、新たに機密情報を再発行してもらう必要がある。

【非特許文献1】電子認証システム推進検討会、“企業間電子商取引システムにおける電子認証システムの仕様に関するガイドライン”、[Online]、[平成16年1月20日検索]、インターネット<URL: <http://www.ecom.or.jp/home/gl2.pdf>>

【発明の開示】

【発明が解決しようとする課題】

【0004】

そのため、ユーザが保持する機密情報を紛失した際には、セキュリティ維持のため、紛失した機密情報を失効させるとともに、機密情報を変更しなければならないという課題がある。また、機密情報を変更するため、再発行まではサービスの提供を受けることができないという課題もある。

【0005】

本発明は、上記の課題を解決するためになされたものであり、ユーザが保持する携帯電話、携帯情報端末、ICカードなどを紛失しても、機密情報を変更することなくサービスの提供を受けることが可能な機密情報管理システム、機密情報管理方法、および機密情報管理プログラムを提供することを目的とする。

【課題を解決するための手段】

【0006】

上記目的を達成するため、請求項1記載の本発明は、利用者の機密情報を管理する機密情報管理システムであって、前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割手段と、前記複数の分割データの一部を、前記利用者が保持するための分割データとして第1の記憶部に記憶させるとともに、前記複数の分割データの残りを、1又は複数の第2の記憶部それぞれに記憶させるデータ記憶手段と、必要に応じて前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割手段で作成された分割データとは異なる複数の分割データを生成するデータ再分割手段と、前記データ再分割手段で作成された前記複数の分割データの一部を前記第1の記憶部に記憶させるとともに、前記第2の記憶部に記憶された各分割データを無効にして、前記データ再分割手段で作成された前記複数のデータの残りを前記第2の記憶部それぞれに記憶させるデータ再記憶手段と、を有することを特徴とする。

【0007】

請求項2記載の本発明は、請求項1記載の発明において、前記機密情報を使用する場合

には、前記利用者が保持する分割データを取得し、該分割データと前記第2の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元手段を有することを特徴とする。

【0008】

請求項3記載の本発明は、請求項2記載の発明において、前記機密情報を使用するときには、使用した事実を使用履歴情報として記憶する使用履歴記憶手段を有することを特徴とする。

【0009】

請求項4記載の本発明は、請求項1記載の発明において、前記機密情報を使用する場合には、前記第2の記憶部に記憶された各分割データのうち、前記所定の個数から前記利用者が保持する分割データの個数を引いた個数の分割データの組み合わせを前記利用者が有する端末に通信ネットワークを介して送信する分割データ送信手段を有することを特徴とする。

【0010】

請求項5記載の本発明は、請求項1乃至4のいずれか1項に記載の発明において、前記第1の記憶部に記憶される分割データを通信ネットワークを介して前記利用者が有する端末に送信する送信手段を有することを特徴とする。

【0011】

請求項6記載の本発明は、請求項1乃至5のいずれか1項に記載の発明において、前記機密情報を前記利用者が有する端末から通信ネットワークを介して受信する受信手段を有することを特徴とする。

【0012】

請求項7記載の本発明は、利用者の機密情報を管理する機密情報管理方法であって、前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割ステップと、前記複数の分割データの一部を、前記利用者が保持するための分割データとして第1の記憶部に記憶させるとともに、前記複数の分割データの残りを、1又は複数の第2の記憶部それぞれに記憶させるデータ記憶ステップと、必要に応じて前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割ステップで作成された分割データとは異なる複数の分割データを生成するデータ再分割ステップと、前記データ再分割ステップで作成された前記複数の分割データの一部を前記第1の記憶部に記憶させるとともに、前記第2の記憶部に記憶された各分割データを無効にして、前記データ再分割ステップで作成された前記複数のデータの残りを前記第2の記憶部それぞれに記憶させるデータ再記憶ステップと、を有することを特徴とする。

【0013】

請求項8記載の本発明は、利用者の機密情報を管理するためのコンピュータが読み取り可能な機密情報管理プログラムであって、前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割ステップと、前記複数の分割データの一部を、前記利用者が保持するための分割データとして第1の記憶部に記憶させるとともに、前記複数の分割データの残りを、1又は複数の第2の記憶部それぞれに記憶させるデータ記憶ステップと、必要に応じて前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割ステップで作成された分割データとは異なる複数の分割データを生成するデータ再分割ステップと、前記データ再分割ステップで作成された前記複数の分割データの一部を前記第1の記憶部に記憶させるとともに、前記第2の記憶部に記憶された各分割データを無効にして、前記データ再分割ステップで作成された前記複数のデータの残りを前記第2の記憶部それぞれに記憶させるデータ再記憶ステップと、前記コンピュータに実行させることを特徴とする。

【発明の効果】

【0014】

本発明に係わる機密情報管理システム、機密情報管理方法、および機密情報管理プログラムによれば、機密情報を秘密分散法を用いて複数に分割して、そのうちの一部をユーザに保持させるので、ユーザが保持する分割情報の紛失があったとしても、残りの分割情報から機密情報を復元できるとともに、秘密分散法を用いて新たに機密情報を再分割し、該再分割情報の一部を新たにユーザに保持させるので、機密情報の変更は不要である。

【0015】

この結果、ユーザが保持する分割情報の紛失があったとしても、機密情報の再発行処理をすることなく、紛失の申告をするだけで、再びサービス提供を受けることができる。

【発明を実施するための最良の形態】

【0016】

以下、本発明の実施の形態を図面を用いて説明する。

【0017】

図1は、本発明の実施の形態に係る機密情報管理システム1が適用されるコンピュータシステム10全体の概略構成を示すブロック図である。

【0018】

図1に示すように、機密情報管理システム1は、インターネット等の通信ネットワーク4を介してユーザが備えるクライアント端末（以下、単に端末とよぶ）2と接続されるとともに、通信ネットワーク4を介して所定のサービスを提供するサービス提供システム5と接続されている。また、機密情報管理システム1は、ハードウェア的に互いに独立した複数（本実施の形態では3とする）のデータ保管用サーバコンピュータ（以下、単に保管サーバとよぶ）3a, 3b, 3cと接続されている。

【0019】

尚、本実施の形態における機密情報とは、ユーザがサービス提供システム5を利用するために必要なパスワード、クレジットカード番号、PKI秘密鍵などの個人情報をいう。

【0020】

上記構成のコンピュータシステム10においては、端末2が所定のサービスをサービス提供システム5から受ける際に必要とされる機密情報Sを機密情報管理システム1に送信すると、機密情報管理システム1において秘密分散法を用いて該機密情報Sを複数のデータに分割し、該分割データを保管サーバ3a, 3b, 3cおよび端末2にそれぞれ送信し、保管させるようになっている。この結果、機密情報Sが機密情報管理システム1に登録されたことになり、ユーザはサービス利用の準備が整ったことになる。尚、図1では、機密情報管理システム1は、端末2からの機密情報Sを4つの分割データD(1), D(2), D(3), D(4)に分割し、それぞれを複数の保管サーバ3a, 3b, 3cおよび端末2に保管するようになっている。

【0021】

また、サービス利用時は、端末2から機密情報管理システム1に対して、ユーザが保持する分割データD(4)を送信すると、機密情報管理システム1は、該分割データD(4)および保管サーバ3a, 3b, 3cの分割データD(1), D(2), D(3)の所定の組み合わせから秘密分散法を用いてもとの機密情報Sを復元し、該機密情報Sをサービス提供システム5に送信するようになっている。これにより、機密情報Sの正当性が確認されれば、ユーザは所定のサービスの提供を受けることができる。

【0022】

機密情報管理システム1は、詳しくは、機密情報Sから秘密分散法を用いて複数の分割データDに分割する分割データ生成部11、複数の分割データDから元データ（機密情報）Sを復元する元データ復元部12、機密情報システム1がサービス提供システム5に機密情報Sを送信した事実をサービス使用履歴として生成する使用履歴生成部13、および端末2、保管サーバ3a, 3b, 3cおよびサービス提供システム5それぞれとデータの送受信を行う通信部14を具備する構成となっている。

【0023】

また、端末2は、ユーザが携行可能な携帯情報端末、携帯電話、ICカードなどの携帯

記憶媒体などが想定されるが、他にモバイルを用途としないコンピュータ機器であってもよいものである。

【0024】

ここで、上述した機密情報管理システム1、端末2、保管サーバ3a, 3b, 3cおよびサービス提供システム5は、それぞれ少なくとも演算機能および制御機能を備えた中央演算装置(CPU)、プログラムやデータを格納する機能を有するRAM等からなる主記憶装置(メモリ)を有する電子的な装置から構成されているものである。また、上記装置およびシステムは、主記憶装置の他、ハードディスクなどの補助記憶装置を具備しているもよい。

【0025】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置またはハードディスクに格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD-ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

【0026】

次に、本実施の形態に係る機密情報管理システム1が適用されるコンピュータシステム10全体の動作について説明する。ここで、図2は、ユーザが機密情報Sを機密情報管理システム1に登録する動作を説明するシーケンス図であり、図3は、ユーザがサービスを利用する時の機密情報管理システム1の動作を説明するシーケンス図であり、図4は、ユーザが保持する分割データDを紛失したときの機密情報管理システム1の動作を説明するシーケンス図である。

【0027】

(1) 機密情報登録処理

まず、ユーザが端末2から通信ネットワーク4を介して機密情報管理システム1に機密情報Sを送信する(ステップS10)。機密情報管理システム1は、機密情報Sを受け取ると、秘密分散法を用いて4つのデータ(分割データ)D(1), D(2), D(3), D(4)に分割する(ステップS20)。

【0028】

ここで、ステップS20の秘密分散法に基づく分割データ生成処理について詳細に説明する。

【0029】

例えば、2次多項式 $F(x) = ax^2 + bx + S \pmod{p}$; p で割った時の余りを表す)を基にしたShamirの秘密分散法{(k, n) 閾値法; 但し、分割数を表す n を4とし、復元できる数を表す k を3とする}で考える。ここで S は元データである機密情報、 $F(x)$ は分割データである。 a, b, p は、機密情報 S の分割に際して任意に決定される。但し、 p は、 a, b, S よりも大きい素数とする。

【0030】

このとき、機密情報管理システム1の分割データ生成処理により、分割データ $F(1), F(2), F(3), F(4)$ {上記分割データ $D(1), D(2), D(3), D(4)$ に対応}は、次式(1)~(4)のように作成される。

【0031】

$$F(1) = a + b + S \pmod{p} \quad \dots (1)$$

$$F(2) = 4a + 2b + S \pmod{p} \quad \dots (2)$$

$$F(3) = 9a + 3b + S \pmod{p} \quad \dots (3)$$

$$F(4) = 16a + 4b + S \pmod{p} \quad \dots (4)$$

この分割データ $F(1), F(2), F(3), F(4)$ の内、 $k=3$ 以上の分割データ {例えば、 $F(1), F(2), F(4)$ } が集まれば、この分割データ

$$F(1) = a + b + S \pmod{p} \quad \dots (1)$$

$$F(2) = 4a + 2b + S \pmod{p} \quad \dots (2)$$

$$F(4) = 16a + 4b + S \pmod{p} \quad \dots (4)$$
を連立して元データ S を求めることができる。そして、 $k-1$ 以下の分割データが集まっても、元データ S を復元することはできない。

【0032】

次に、機密情報管理システム 1 は、このようにして生成された分割データを各保管サーバ 3 a, 3 b, 3 c および端末 2 にネットワーク 4 を介して送信する (ステップ S 30)。

【0033】

次に、保管サーバ 3 a, 3 b, 3 c は、それぞれ送信されてきた分割データ $D(1)$, $D(2)$, $D(3)$ をハードディスク等の記憶装置に記憶する (ステップ S 40)。また、端末 2 は、送信されてきた分割データ $D(4)$ をハードディスク等の記憶装置に記憶する (ステップ S 50)。

【0034】

これにより、端末 2、保管サーバ 3 a, 3 b, 3 c のうちいずれか 1 つの分割データに紛失、破壊等があっても、残りの 3 つの分割データからもとの機密情報 S を復元できる (Shamir の秘密分散法において分割数を 4 とし、復元できる数を 3 とする場合)。

【0035】

(2) サービス利用処理

ユーザがサービス提供システム 5 を利用する場合には、まず、端末 2 に保持する分割データ $D(4)$ を通信ネットワークを介して機密情報管理システム 1 に送信する (ステップ S 10)。

【0036】

機密情報管理システム 1 は、端末 2 から分割データ $D(4)$ を受け取ると、残りの分割データ $D(1)$, $D(2)$ を保管サーバ 3 に要求し (Shamir の秘密分散法にて分割数を 4 とし、復元できる数を 3 とする場合)、該分割データ $D(1)$, $D(2)$ を受け取る (ステップ S 120)。尚、この場合には、3 つの分割データは任意の組み合わせでよく、例えば、上述したように $D(1)$, $D(2)$, $D(4)$ の組み合わせの他、 $D(1)$, $D(2)$, $D(3)$ の組み合わせ、 $D(1)$, $D(3)$, $D(4)$ の組み合わせ、 $D(2)$, $D(3)$, $D(4)$ の組み合わせのいずれでもよい。

【0037】

次に、機密情報管理システム 1 は、分割データ $D(1)$, $D(2)$, $D(4)$ から秘密分散法を用いて機密情報 S を復元する (ステップ S 130)。そして、復元した機密情報 S をサービス提供システム 5 に送信して (ステップ S 140)、機密情報 S を復元し送信した事実を使用履歴として生成する (ステップ S 150)。

【0038】

サービス提供システム 5 は、機密情報管理システム 1 から機密情報 S を受け取ると、該機密情報 S の正当性を判断して、端末 2 に通信ネットワーク 4 を介してサービス提供を行う (ステップ S 160, S 170)。これにより、ユーザは所望のサービスの提供を受けることができる。

【0039】

(3) 分割データ紛失時処理

ユーザが分割データ $D(4)$ を紛失した場合 (例えば、分割データ $D(4)$ を記憶している端末 2 を紛失した場合) には、まず、機密情報管理システム 1 にその旨を申告する (例えば、機密情報管理システム 1 の運用者へ電話連絡する) (ステップ S 210)。

【0040】

これにより、機密情報システム 1 は、保管サーバ 3 a, 3 b, 3 c に分割データを要求し、保管サーバ 3 a, 3 b, 3 c からそれぞれ分割データ $D(1)$, $D(2)$, $D(3)$ を受け取る (Shamir の秘密分散法にて分割数を 4 とし、復元できる数を 3 とする場合) (ステップ S 220)。

【0041】

次に、機密情報管理システム 1 は、分割データ $D(1)$, $D(2)$, $D(3)$ から秘密分散法を用いて

機密情報Sを復元する(ステップS230)。そして、復元した機密情報Sを、再び秘密分散法を用いて新たに4つのデータ(分割データ)D'(1),D'(2),D'(3),D'(4)に分割する(ステップS240)。

【0042】

ここで、分割データD'(1),D'(2),D'(3),D'(4)は、それぞれ最初に生成された分割データD(1),D(2),D(3),D(4)とは異なるデータで、具体的には、上述した2次多項式 $F(x) = ax^2 + bx + S$ において、最初の分割時におけるaおよびbとは異なるa'およびb'を用いて生成された分割データである。

【0043】

次に、機密情報管理システム1は、このようにして生成された再分割データを各保管サーバ3a, 3b, 3cおよび端末2(例えば、ユーザが分割データD(4)を記憶している端末2を紛失した場合には、ユーザが新たに購入した端末2)にネットワーク4を介して送信する(ステップS250)。

【0044】

次に、保管サーバ3a, 3b, 3cは、それぞれ送信されてきた再分割データD'(1),D'(2),D'(3)をハードディスク等の記憶装置に記憶する(ステップS260)。また、端末2は、送信されてきた分割データD'(4)をハードディスク等の記憶装置に記憶する(ステップS270)。これにより、ユーザは再びサービス利用が可能となる。

【0045】

従って、本実施の形態によれば、所定のサービスを受ける際に必要とされる機密情報Sを秘密分散法を用いて複数に分割して、そのうちの一部をユーザに保持させるので、ユーザが保持する分割データの紛失があったとしても、残りの分割データから機密情報を復元できるとともに、秘密分散法を用いて新たに機密情報を再分割し、該再分割データの一部を新たにユーザに保持させるので、機密情報Sの変更は不要である。

【0046】

この結果、ユーザが保持する分割データの紛失があったとしても、機密情報Sの再発行処理をすることなく、紛失の申告をするだけで、再びサービス提供を受けることができる。

【0047】

また、紛失した分割データを取得した第3者が機密情報管理システム1にアクセスしても機密情報Sを復元することができないので、サービスを利用することができず、安全性が確保される。

【0048】

さらに、ユーザの使用履歴が機密情報管理システム1に保管されるので、ユーザが分割データを紛失してから紛失した旨を申告するまでの間に、仮に第3者が分割データを取得してサービスを悪用したとしても、使用履歴により悪用の有無を判別することができる。

【0049】

以上、本発明の実施の形態について説明してきたが、本発明の要旨を逸脱しない範囲において、本発明の実施の形態に対して種々の変形や変更を施すことができる。例えば、上記実施の形態においては、端末2から機密情報Sの機密情報管理システム1への受け渡しを通信ネットワーク4を介して行ったが、本発明はこれに限定されず、例えば、機密情報Sを記録した記録媒体を郵送など通信ネットワーク3以外の手段を介して受け渡してもよい。また、同様に、ユーザが保持する分割データも通信ネットワーク4を介して受け取ったが、本発明はこれに限定されず、例えば、分割データを記録した記録媒体を郵送など通信ネットワーク3以外の手段を介して受け取ってもよい。

【0050】

また、上記実施の形態によれば、秘密分散法としてShamirの秘密分散法{(k, n) 閾値法; 但し、分割数を表すnを4とし、復元できる数を表すkを3とする}を用いたが、本発明はこの構成に限定されるものではなく、上記実施の形態で述べた分割数以外の他の分割数、および上記実施の形態で述べた秘密分散法以外の他の秘密分散法を用いるこ

とも可能である。

【0051】

また、上記実施の形態においては、ユーザがサービス利用時には、機密情報管理システム1が機密情報を復元したが、本発明はこれに限定されず、ユーザの端末2が、端末2に記憶される分割データと機密情報管理システム1から取得した分割データから、秘密分散法を用いて機密情報を復元し、該機密情報をサービス提供システム5に送信してもよいものである。尚、この場合には、復元された機密情報が端末2に記憶されたままユーザが端末2を紛失すると、本発明が解決しようとする課題が解決できないことになるため、該機密情報をサービス提供システム5に送信後すぐに端末2から消去する仕組み、あるいは、端末2のデータの第三者による不正な取り出しを防止する仕組みなどを備えることが必要である。

【0052】

さらに、上記実施の形態においては、ユーザからの要求により再分割処理を行ったが、機密情報管理システム1が自発的に所定の契機により再分割処理を行ってもよいものである。

【図面の簡単な説明】

【0053】

【図1】本発明の実施の形態に係る機密情報管理システムが適用されるコンピュータシステム全体の概略構成を示すブロック図である。

【図2】本発明の実施の形態に係る機密情報管理システムにおいて機密情報を登録する処理を説明するシーケンス図である。

【図3】本発明の実施の形態に係る機密情報管理システムにおいてサービス利用時の処理を説明するシーケンス図である。

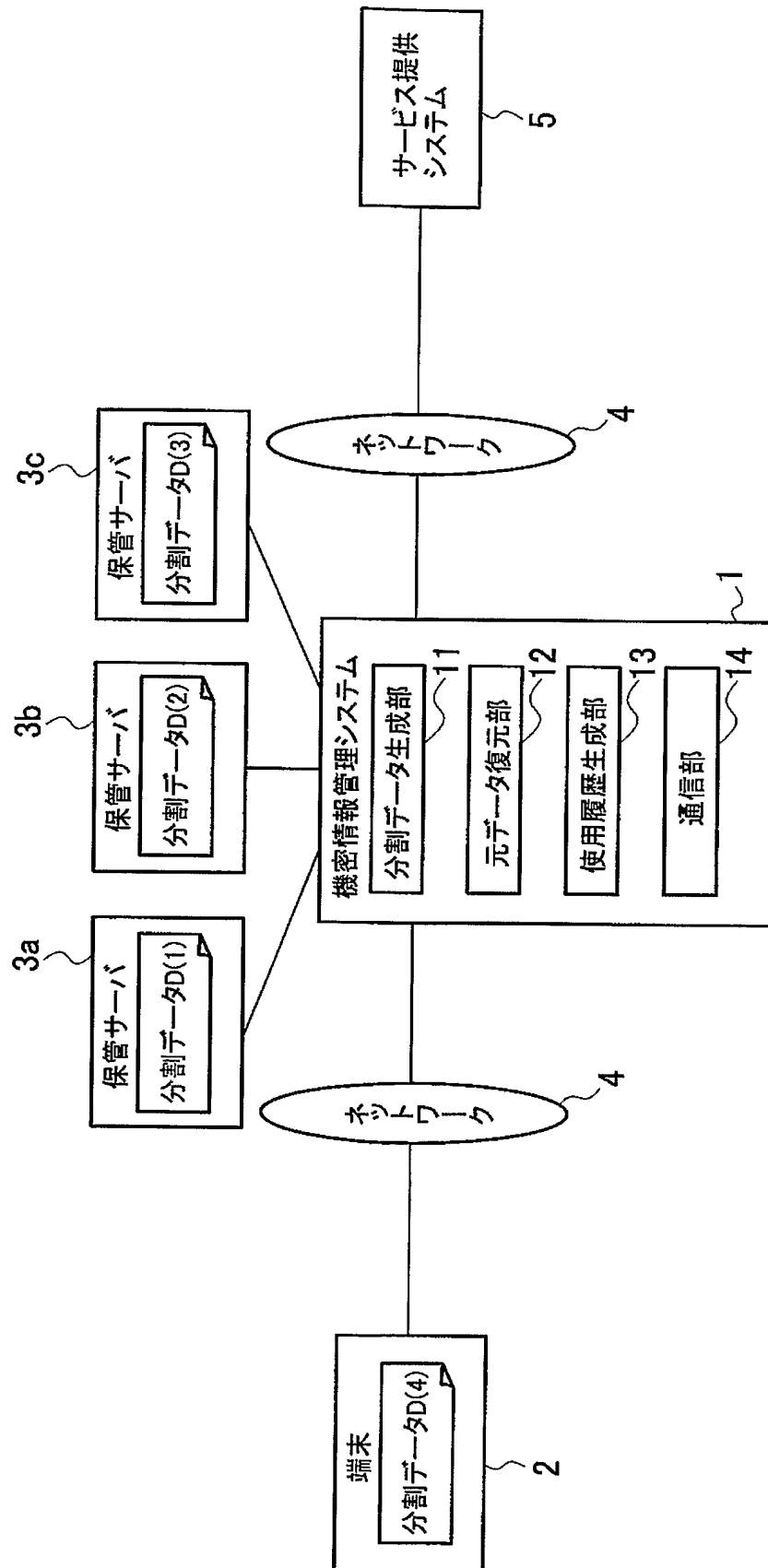
【図4】本発明の実施の形態に係る機密情報管理システムにおいてユーザが保持する機密情報の一部を紛失したときの処理を説明するシーケンス図である。

【符号の説明】

【0054】

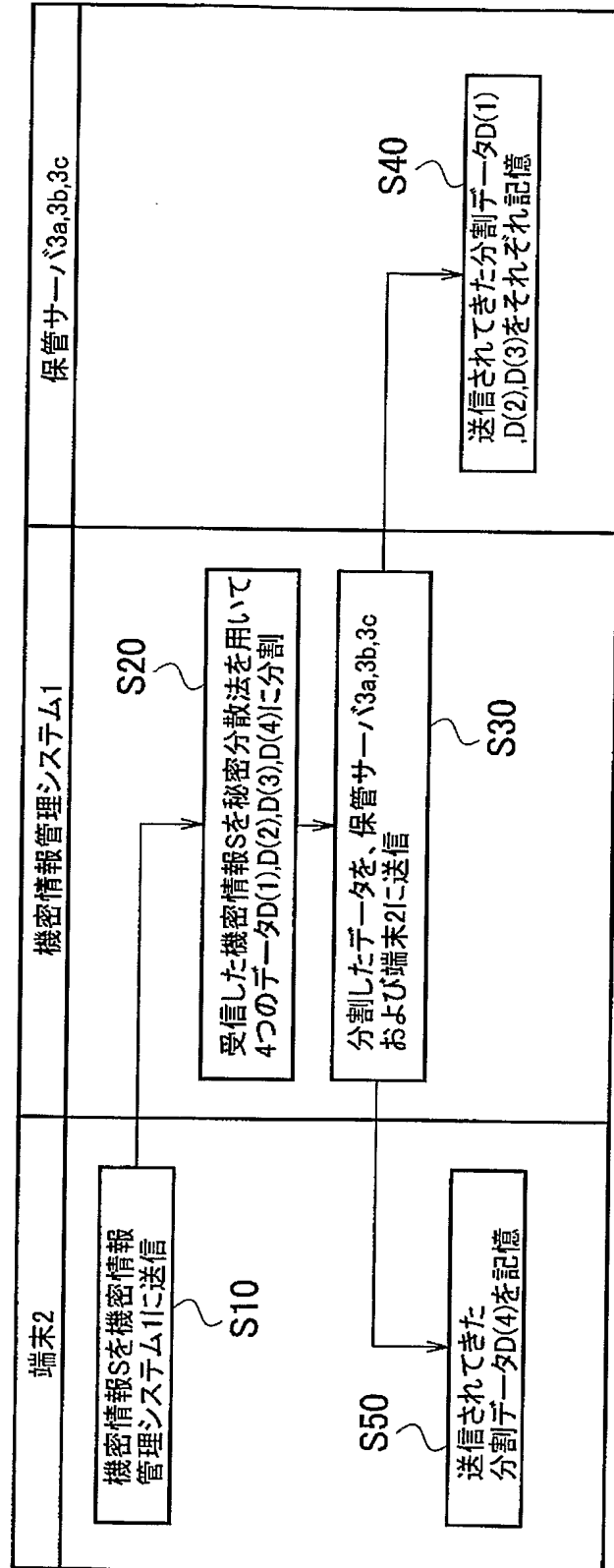
- 1…機密情報管理システム
- 2…端末
- 3 a, 3 b, 3 c…保管サーバ
- 4…通信ネットワーク
- 5…サービス提供システム
- 10…コンピュータシステム
- 11…分割データ生成部
- 13…元データ復元部
- 15…使用履歴生成部
- 17…通信部

【書類名】 図面
【図 1】

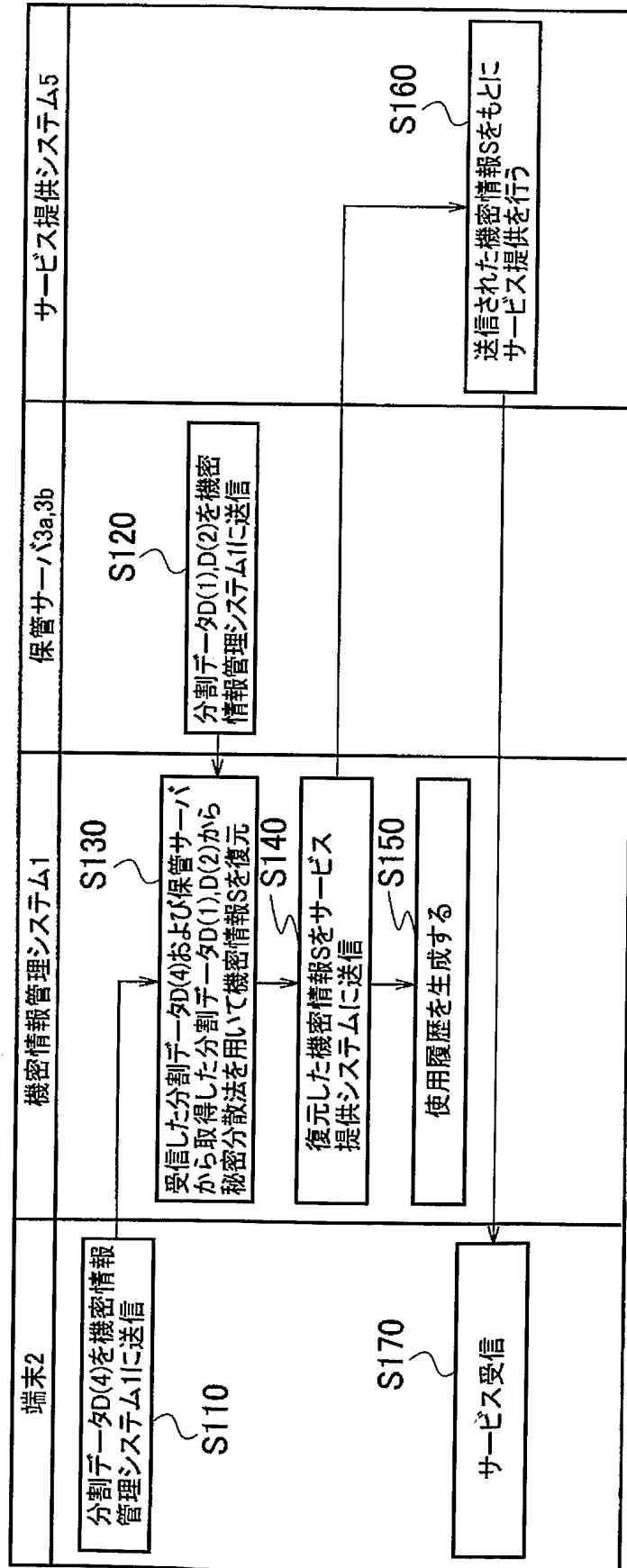


10

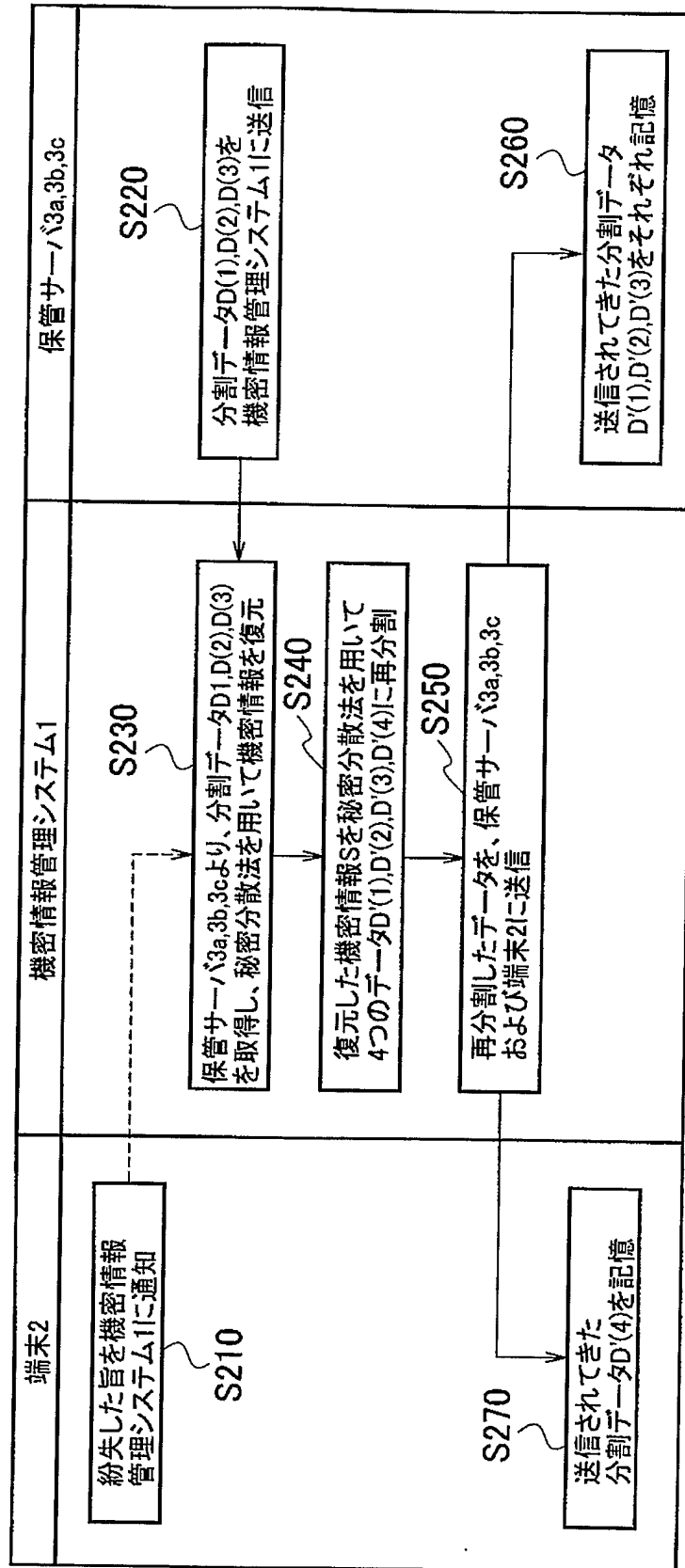
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 ユーザが保持するサービス利用のための情報を紛失しても、機密情報を変更することなくサービスの提供を受けることができる。

【解決手段】 端末2が機密情報Sを機密情報管理システム1に送信すると、機密情報管理システム1は秘密分散法を用いて機密情報Sを複数のデータに分割し、分割データを保管サーバ3a, 3b, 3c及び端末2に保管させる。サービス利用時は、端末2から分割データを機密情報管理システム1に送信すると、機密情報管理システム1は、該分割データおよび保管サーバの分割データから秘密分散法を用いて機密情報Sを復元し、機密情報Sをサービス提供システム5に送信する。ユーザが分割データを紛失した際は、機密情報管理システム1は、保管サーバ3a, 3b, 3cの分割データから秘密分散法を用いて機密情報Sを復元し、機密情報Sを再分割して、該再分割データを保管サーバ3a, 3b, 3c及び端末2に保管させる。

【選択図】 図1



特願 2 0 0 4 - 0 3 3 3 5 5

ページ： 1/E

出 願 人 履 歴 情 報

識別番号

[3 9 9 0 3 5 7 6 6]

1. 変更年月日

1 9 9 9 年 6 月 9 日

[変更理由]

新規登録

住 所

東京都千代田区内幸町一丁目 1 番 6 号

氏 名

エヌ・ティ・ティ・コミュニケーションズ株式会社